



패스키: 비밀번호가 필요 없는 미래를 향한 발걸음

국가 주도 사이버 공격을 비롯한 온라인상에서의 악성 이용자가 극적으로 증가함에 따라, Google은 모두에게 더 안전한 세상을 만들기 위해 Google의 전문지식을 공유하고, 사회에 공헌하며, 최첨단 사이버 보안의 발전을 위해 지속적으로 노력하는 등 그 어느 때보다도 사람, 기업, 정부를 보호하는 데 집중하고 있습니다.

오늘날 비밀번호는 온라인 보안에 필수적인 요소이지만 피싱과 같은 위협은 날로 커지고 있습니다. Google은 오랜 시간 이러한 문제를 인식하고 2단계 인증(2SV), Google 비밀번호 관리자, 보안 키 그리고 패스키 등 인증 도구의 사용을 권장하고 있습니다.

당면과제

비밀번호는 컴퓨터에서 60년 이상 사용되어 왔으나 오늘날 이용자와 조직의 데이터를 안전하게 지키는 데는 충분한 역할을 하지 못하고 있습니다. 피싱 공격은 비밀번호의 보안 취약성을 이용해 그 규모와 복잡성을 계속 키우고 있습니다. 그 예는 다음과 같습니다.

- ✔ 2021년 정보 유출의 60% 이상이 인증 정보 유출 또는 피싱으로 인해 발생하였습니다.¹
- ✔ 2022년 피싱으로 인한 정보 유출로 인해 조직이 지출한 금액은 평균 491만 달러입니다.²
- ✔ 2022년 피싱 공격은 61% 증가해 6개월 동안 총 2억 5,500만 건에 도달했습니다.³

2단계 인증(2SV/2FA)이 도움이 될 수 있으나 추가적인 번거로움으로 인해 이용자에게 부담을 줄 수 있으며 문자 인증의 경우 'SIM 교체'와 같은 피싱 및 표적 공격을 완전히 차단할 수는 없습니다.

해결방안

Google은 이제 FIDO Alliance와의 협업을 통해 패스키를 지원합니다. 더 간단하고 안전한 방식의 비밀번호 대체재로 전 세계 수십억 이용자에게 피싱 방지 기술을 제공할 수 있습니다. 이용자는 패스키를 사용하여 지문과 얼굴 인식, 또는 화면 잠금으로 더 편리하고 안전한 로그인 경험을 경험하는 동시에 비밀번호 입력 과정을 생략할 수 있습니다.

패스키는 2023년 초부터 개인 Google 계정 및 900만 명 이상의 Google Workspace 사용자, Chrome과 Android의 서드 파티 사이트 및 앱에서 사용할 수 있습니다.



가장 간단하고 빠른 로그인 방법

패스키는 기억하거나 입력할 필요가 없어 **4배 더 간단합니다**. 이용자의 모든 기기에서 지문, 얼굴 인식, 화면 잠금 방식으로 로그인할 수 있습니다.

차세대 계정 보안

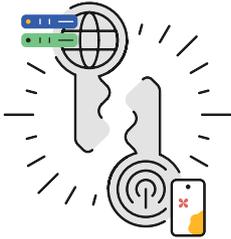
패스키는 피싱 등의 위협에 대항하는 고도의 강력한 보안을 제공합니다. 또한 패스키는 로컬 기기에 저장되기 때문에 공격자가 추측하거나 재사용할 수 없어 이용자의 정보를 안전하게 지킬 수 있습니다.

이용자 개인정보보호

패스키는 이용자의 개인 기기에 비공개로 저장되며 Google이나 제 3자 파트너에게 공유되지 않습니다. 지문, 얼굴 인식, 화면 잠금을 사용하면 비공개 키에 접근하는 사람이 이용자 본인이라고 인증할 수 있습니다.



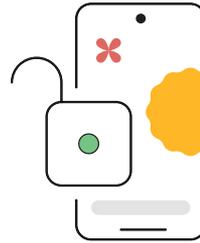
패스키 작동 원리



패스키는 로그인하려는 웹사이트 서버의 공개 키와 이에 상응하는 사용자 기기의 비공개 키, 이렇게 두 부분으로 이루어져 있습니다.



로그인할 때 웹사이트는 이용자의 공개 키가 비공개 키와 일치하는지 확인합니다.



이 과정에서 이용자는 기기를 잠금 해제하기만 하면 됩니다.



그러면 이용자는 로그인에 성공하며, 비공개 키와 생체 인식 데이터는 안전하게 사용자 기기에 저장되어 그 어디에도 공유되지 않습니다.

더 안전한 생태계 만들기

기업과 정부부처의 패스키 활용

패스키는 이용자에게 의미 있는 보안 및 유용성을 제공합니다. Google은 이 기술의 최초 주요 퍼블릭 클라우드 제공업체로서 중소기업과 대기업, 학교와 정부에 이르는 고객들에게 제공할 수 있게 되어 대단히 기쁩니다.

인터넷에서 비밀번호 없이도 더 안전하게 로그인하기 위한 파트너십

Google은 Chrome 및 Android 플랫폼 전반에서 패스키를 사용할 수 있도록 여러 브랜드와 파트너십을 맺어 해당 브랜드 이용자들에게 더 간단하고 안전한 로그인 환경을 제공하고 있습니다. 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal, Yahoo! Japan과 같이 전자 상거래, 금융 기술, 여행 등 여러 산업 전반의 파트너들이 이미 비밀번호가 필요 없는 미래를 위한 여정에 함께하고 있습니다.

비밀번호가 필요 없는 미래를 위한 Google의 여정

패스키는 Google이 10년 넘게 계획하고 만들어 온 비밀번호 없는 미래에 더 가까워지는 열쇠입니다.

2008	2011	2012	2013	2014	2017	2019	2023
더 간단하고 안전한 로그인을 위한 Google 비밀번호 관리자 런칭	Google 계정에 2단계 인증 (2SV) 활성화	Google 직원을 위한 피싱 방지 보안 키 도입	비밀번호 없는 세계로의 개방형 표준을 이끌고자 FIDO Alliance에 가입	모두를 위한 피싱 방지 보안 키 확장	고위험 이용자를 위한 고급 보호 프로그램(APP) 도입	웹사이트 전반에서의 비밀번호 없는 재인증을 위해 Android의 FIDO 지원 확장	Google 계정, Chrome 및 Android의 Workspace 고객과 제 3자 파트너에 패스키 활성화

패스키로 전환하는 과정에서도 비밀번호는 계속 우리 삶의 일부를 차지하겠지만, Google은 이용자와 업계 관계자 모두를 지원하며 다음 단계로의 도약을 통해, Google로 모두가 더 안전하면서도 간단하게 로그인할 수 있도록 노력하겠습니다.

출처: 1 - Verizon Data Breach Investigation report 2022 | 2 - IBM Cost of Data Breach report 2023
3 - CNBC's Cyber Report | 4 - Google Security Blog, May 2023